PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

HASHIMOTO, et al.	Group Art Unit: Not yet assigned
Application No.: New	Examiner: Not yet assigned
Filed: Concurrently Herewith	Attorney Dkt. No.: 108391-00038

For: **MEMORY DEVICE, MEMORY ACCESS LIMITING SYSTEM, AND MEMORY ACCESS METHOD**

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: March 24, 2004

Sir:

The benefit of the filing dates of the following prior foreign application(s) in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

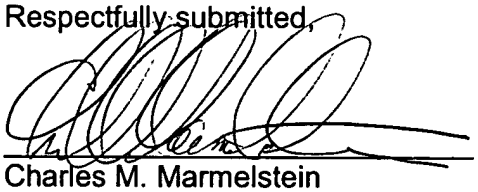
Japanese Patent Application No. 2003-097401 filed on March 31, 2003

In support of this claim, certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these/this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Deposit Account No. 01-2300.

Respectfully submitted,



Charles M. Marmelstein
Registration No. 25,895

Customer No. 004372
ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
1050 Connecticut Avenue, N.W.,
Suite 400
Washington, D.C. 20036-5339
Tel: (202) 857-6000
Fax: (202) 638-4810
CMM/jch

F503-009-05

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月３１日

出願番号
Application Number: 特願２００３－０９７４０１

[ST. 10/C]: [ＪＰ２００３－０９７４０１]

出願人
Applicant(s): 富士通株式会社
株式会社エフ・エフ・シー

２００３年１１月２６日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９７７９１

【書類名】　特許願
【整理番号】　0251753
【提出日】　平成15年 3月31日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/14
【発明の名称】　メモリ装置、メモリアクセス制限システムおよびメモリアクセス方法
【請求項の数】　10
【発明者】
【住所又は居所】　東京都日野市富士町１番地　株式会社エフ・エフ・シー内
【氏名】　橋本　勝彦
【発明者】
【住所又は居所】　東京都日野市富士町１番地　株式会社エフ・エフ・シー内
【氏名】　大久保　博
【発明者】
【住所又は居所】　東京都日野市富士町１番地　株式会社エフ・エフ・シー内
【氏名】　清田　昌紀
【発明者】
【住所又は居所】　東京都日野市富士町１番地　株式会社エフ・エフ・シー内
【氏名】　三石　俊二
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　升谷　江一

【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【特許出願人】
　【識別番号】　000237156
　【氏名又は名称】　株式会社エフ・エフ・シー
【代理人】
　【識別番号】　100104190
　【弁理士】
　【氏名又は名称】　酒井　昭徳
【手数料の表示】
　【予納台帳番号】　041759
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9906241
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　メモリ装置、メモリアクセス制限システムおよびメモリアクセス方法

【特許請求の範囲】

【請求項１】　データの読み出しおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第１のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域と、

前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みをおこなう制御部と、

を具備することを特徴とするメモリ装置。

【請求項２】　前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとを比較する比較部をさらに具備することを特徴とする請求項１に記載のメモリ装置。

【請求項３】　前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第１のデータ領域に対するデータの読み出しおよび書き込みを禁止することを特徴とする請求項２に記載のメモリ装置。

【請求項４】　データの読み出しおよび書き込みが可能で、前記第２のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第４のデータ領域をさらに具備することを特徴とする請求項１～３のいずれか一つに記載のメモリ装置。

【請求項５】　データの読み出しおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第１のデータ領域、データの書き込みが可能で

、かつデータの読み出しが不可能な不揮発性の第２のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域、並びに前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みをおこなう制御部を備えたメモリ装置と、

前記第１のデータ領域および前記第２のデータ領域にデータを書き込む書き込み手段と、

前記書き込み手段と前記メモリ装置との間のデータの授受に供せられる第１のインターフェース手段と、

前記第３のデータ領域にデータを書き込むとともに、前記第１のデータ領域に対するデータの読み出しまたは書き込みのアクセスをおこなう読み書き手段と、

前記読み書き手段と前記メモリ装置との間のデータの授受に供せられる第２のインターフェース手段と、

を具備することを特徴とするメモリアクセス制限システム。

【請求項６】　前記メモリ装置は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとを比較する比較部をさらに備えていることを特徴とする請求項５に記載のメモリアクセス制限システム。

【請求項７】　前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第１のデータ領域に対するデータの読み出しおよび書き込みを禁止することを特徴とする請求項６に記載のメモリアクセス制限システム。

【請求項８】　前記メモリ装置は、データの読み出しおよび書き込みが可能で、前記第２のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第４のデータ領域をさらに備えていることを特徴とする請求項５～７のいずれか一つに記載のメモリアクセス制限システム。

【請求項９】　リセット後に、データの読み出しおよび書き込みが可能な不揮発性の第１のデータ領域に暗号化されていない所定のデータを書き込むとも

に、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域にキーデータを書き込み、前記第１のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態にする第１の工程と、

前記第１のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態のときに、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域に仮のキーデータを書き込む第２の工程と、

前記仮のキーデータが前記キーデータに一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、一方、前記仮のキーデータが前記キーデータと異なるときに前記第１のデータ領域に対するデータの読み出しおよび書き込みを禁止する第３の工程と、

を含むことを特徴とするメモリアクセス方法。

【請求項１０】　前記第２の工程の前に、

データの読み出しおよび書き込みが可能な不揮発性の第４のデータ領域に、前記キーデータを暗号化して書き込む第４の工程と、

前記第４のデータ領域に格納されている暗号データを読み出し、該暗号データを復号化して前記キーデータを取得する第５の工程と、

をさらに有し、

前記暗号データの復号化により得られたキーデータを、前記第２の工程において仮のキーデータとして前記第３のデータ領域に書き込むことを特徴とする請求項９に記載のメモリアクセス方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＣを内蔵したメモリ装置、ＩＣを内蔵したメモリ装置へのアクセス制限システム、およびＩＣを内蔵したメモリ装置へのアクセス方法に関し、特に、ＩＣを内蔵したメモリ装置のメモリに記憶された秘密のデータを秘匿する技術に関する。

【０００２】

航空貨物には、送り先などの管理をおこなうために、国際航空運送協会（ＩＡ

ＴＡ）によるＩＡＴＡコードが記されたタグが取り付けられる。一方、ＩＣを内蔵したメモリカード（以下、ＩＣカードとする）は、持ち運びが容易であるという可搬性と、搬送先でのデータの読み出しや書き込みが容易であるという利便性を兼ね備えている。

【０００３】

そこで、タグの代わりとしてＩＣカードを用い、ＩＣカードに、荷主の情報、内容物の情報、発着空港の情報、経由地の情報など、より多くの情報を記憶させ、それらの情報の改ざんを防ぐことによって、現状よりもさらに運航上の安全性や、荷物が送り先に届く確実性を高めることができると考えられる。また、航空貨物の管理に限らず、たとえば個人情報などを記憶したＩＣカードにおいては、秘密にすべき情報が漏洩したり、改ざんされるのを防ぐ必要がある。

【０００４】

【従来の技術】

ＩＣカードに記憶された秘密のデータを盗み見られたり、改ざんされるのを防ぐには、ＩＣカードにデータを暗号化して保存しておくのが有効である。また、ＩＣカードにおいて、内蔵するメモリにパスワードを記憶させておき、このパスワードに一致する外部入力があるときに、メモリへのアクセスを許可する構成としたものが公知である（特許文献１参照）。この特許文献１に開示されたＩＣカードでは、メモリの良否をテストする場合などに、外部入力がパスワードに一致していなくても、メモリにアクセスすることができる。

【０００５】

【特許文献１】

特開平９－２０４３６１号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、ＩＣカードを航空貨物のタグ代わりに用いる場合、以下に述べる理由により、データの暗号化は好ましくない。航空貨物は、空港でベルトコンベア等に載せられて自動搬送される。そして、航空貨物がゲートを通過する際に、ゲートに備え付けられたアンテナからＩＣカードに電力が供給される。その電

力によりＩＣカードが駆動され、電磁誘導方式によりＩＣカードに対してデータの読み出しまたは書き込みがおこなわれる。

【０００７】

つまり、航空貨物がゲートを通過している間に、ＩＣカードのメモリに対して、データを暗号化して書き込む処理や、データを復号化して読み出す処理が完了しなければならない。しかし、データの暗号化および復号化には時間がかかるため、ＩＣカードがゲートを通過するわずか１秒にも満たない時間（ミリ秒オーダ）内に、データの書き込みや読み出しの処理を完了させるのは困難である。

【０００８】

本発明は、上記問題点に鑑みてなされたものであって、ＩＣカードにデータを暗号化することなく記憶させ、その記憶データの漏洩や改ざんを防ぐことができるメモリ装置を提供することを目的とする。また、本発明は、ＩＣカードに対する、暗号化していないデータの読み出しや書き替えを制限したメモリアクセス制限システムを提供することを目的とする。さらに、本発明は、ＩＣカードに記憶された、暗号化していないデータの盗み見や改ざんのためのアクセスを禁止したメモリアクセス方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本発明は、メモリ装置（ＩＣカード）に、データの読み出しおよび書き込みが可能な不揮発性の第１のデータ領域（データ領域）と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域（キーデータ領域）と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域（キーレジスタ）を設ける。そして、第１のデータ領域（データ領域）に暗号化されていない秘密にすべき所定のデータを書き込むとともに、第２のデータ領域（キーデータ領域）にキーデータを書き込むことによって、第１のデータ領域（データ領域）に対するデータの読み出しおよび書き込みが禁止された状態となる。第１のデータ領域（データ領域）に対するデータの読み出しまたは書き込みは、第３のデータ領域（キーレジスタ）に正しいキーデータが書き込まれたときに許可され、間違ったキーデータ

が書き込まれたときに禁止される。

【００１０】

この発明において、メモリ装置（ＩＣカード）に、データの読み出しおよび書き込みが可能な不揮発性の第４のデータ領域（暗号レジスタ）を設け、この第４のデータ領域（暗号レジスタ）に、キーデータを暗号化して書き込んでおき、メモリ装置（ＩＣカード）を受け取った者が、第４のデータ領域（暗号レジスタ）に格納されている暗号データを読み出して復号化することにより正しいキーデータを取得することができる構成としてもよい。

【００１１】

この発明によれば、正しいキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが許可され、間違ったキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが禁止される。また、秘密データは、メモリ装置に暗号化されずに記憶される。また、キーデータを読み出すことは不可能である。

【００１２】

【発明の実施の形態】

以下に、本発明の実施の形態について図面を参照しつつ詳細に説明する。なお、本実施の形態においては、メモリ装置を構成するＩＣカードを送る側を送り手とし、受け取る側を受け手と表す。

【００１３】

（実施の形態１）

図１は、本発明にかかるＩＣカードの構成の一例を示すブロック図であり、図２は、ＩＣカードへのアクセス制限システムの概略構成の一例を示す模式図である。

【００１４】

図１および図２において、符号１はＩＣカードである。符号２は、書き込み手段を構成し、ＩＣカード１の送り手側のホストとなるコンピュータである。符号３は、読み書き手段を構成し、ＩＣカード１の受け手側のホストとなるコンピュータである。符号４および５は、それぞれＩＣカード１の送り手側および受け手

側のリーダ／ライタである。リーダ／ライタ４，５は、ＩＣカード１に対するデータの読み出しまたは書き込みをおこなう際のデータの授受に供せられるインターフェース手段であり、それぞれのホストコンピュータ２，３に接続されている。

【００１５】

図２に示すように、ＩＣカード１の送り手は、コンピュータ２を操作し、リーダ／ライタ４を介してＩＣカード１へアクセスして、後述するキーデータの登録、ＩＣカード１のメモリへのデータの書き込み、キーデータの暗号化などの処理をおこなう。一方、ＩＣカード１の受け手は、コンピュータ３を操作し、ＩＣカード１へアクセスして、キーデータの認証、ＩＣカード１のメモリからのデータの読み込み、暗号化されたキーデータの復号化などの処理をおこなう。

【００１６】

図１に示すように、ＩＣカード１は、メモリ１１、キーデータ領域（第２のデータ領域）１２、データ領域（第１のデータ領域）１３、キーレジスタ（第３のデータ領域）１４、比較部１５、キーデータ設定フラグ（第５のデータ領域）１６、暗号レジスタ（第４のデータ領域）１７、リード／ライト制御部（制御部）１８および通信部１９を備えている。メモリ１１は、読み出しおよび書き替えが可能な不揮発性のメモリ、たとえば強誘電性メモリや、読み出しおよび書き替えが可能な読み出し専用メモリ、たとえば電気的に一括消去可能なフラッシュメモリや電気的に消去可能なＥＥＰＲＯＭなどにより構成される。

【００１７】

メモリ１１は、キーデータを格納するキーデータ領域１２と、送り手または受け手によりデータの書き込みまたは読み出しが可能なデータ領域１３を備えている。特に限定しないが、たとえばメモリ１１は２５４ブロックで構成されており、そのうちの１ブロックがキーデータ領域１２として割り振られ、残りがデータ領域１３となる。メモリ１１に対するデータの読み出しまたは書き込みは、ブロック単位で実施される。

【００１８】

キーデータは、データ領域１３へのアクセスの許可または禁止の設定をおこな

うためのパスワードである。キーデータは、送り手がキーデータ登録処理を実行したときに、リーダ／ライタ４から通信部１９を介してリード／ライト制御部１８へ送られ、リード／ライト制御部１８の書き込み制御によりキーデータ領域１２に書き込まれる。キーデータ領域１２に対しては、データの書き替えのみをおこなうことができる。つまり、キーデータ領域１２にキーデータを書き込むことはできるが、書き込まれたキーデータをキーデータ領域１２から読み出すことはできない。

【００１９】

キーレジスタ１４は、キーデータ領域１２に書き込まれたキーデータと比較されるデータを格納する領域である。送り手または受け手がキーデータ認証処理時に入力したデータは、リーダ／ライタ４，５から通信部１９を介してキーレジスタ１４に書き込まれる。キーレジスタ１４に格納されたデータを読み出すことはできない。キーレジスタ１４に対するデータの書き替えのみが可能である。

【００２０】

比較部１５は、キーデータ領域１２に格納されているキーデータと、キーレジスタ１４に格納されているデータとの比較をおこなう。比較の結果が一致であれば、メモリ１１および暗号レジスタ１７に対してイネーブル信号がアサートされ、データ領域１３のアクセスおよび暗号レジスタ１７のアクセスが許可される。不一致の場合には、イネーブル信号がネゲートされ、データ領域１３のアクセス禁止、および暗号レジスタ１７に対するライトが禁止される。

【００２１】

キーデータ設定フラグ１６は、キーデータ領域１２に対するキーデータの書き込み処理が実行されたときに、たとえばリード／ライト制御部１８の書き込み制御によりセットされる。キーデータ設定フラグ１６がセットされているときには、比較部１５における２つのデータの比較、および比較結果に基づいたメモリ１１に対するイネーブル信号のアサートまたはネゲートが有効となり、上述したように、データ領域１３へのアクセスが許可または禁止される。キーデータ設定フラグ１６がセットされていない状態、すなわちキーデータ領域１２にキーデータが書き込まれていない状態のときには、比較部１５から出力されるイネーブル信

号は常にアサートされ、データ領域１３へのアクセスは許可される。

【００２２】

暗号レジスタ１７は、暗号化されたキーデータ（以下、暗号データとする）を格納する領域である。送り手がキーデータの暗号化処理を実行すると、キーデータは、コンピュータ２（図２参照）により暗号化される。その暗号データは、リーダ／ライタ４から通信部１９を介して暗号レジスタ１７に書き込まれる。暗号レジスタ１７に対しては、暗号データの書き込みだけでなく、読み出しもおこなうことができる。受け手は、暗号レジスタ１７に格納された暗号データを、通信部１９を介してリーダ／ライタ５で読み込み、コンピュータ３（図２参照）により復号化することによって、キーデータ領域１２に格納されているキーデータを知ることができる。この際、比較部１５は、暗号化レジスタ１７への書き込みは、キーデータ領域１２と、キーレジスタ１４のデータが同じ場合のみおこなわせる。暗号化レジスタ１７からの読み出しは、キーデータ領域１２とキーレジスタ１４のデータが同じでも異なっていても可能にする。

【００２３】

リード／ライト制御部１８は、キーデータ領域１２およびデータ領域１３に対するデータの書き込みおよび読み出しの制御をおこなう。通信部１９は、リーダ／ライタ４，５との間で、たとえば接触式であれば電気的に、あるいは非接触式であれば電磁誘導方式により、データの授受をおこなう。また、通信部１９は、リーダ／ライタ４，５から、ＩＣカード１を駆動するための電力の供給を受ける。

【００２４】

つぎに、上述した構成のＩＣカードへのアクセス方法について説明する。図３は、実施の形態１にかかるＩＣカードへのアクセス方法を説明するフローチャートである。また、図４および図５は、そのアクセス方法の実行時のメモリ状態を示す模式図である。また、図６および図７は、ＩＣカードとキーデータの授受形態を示す模式図である。

【００２５】

まず、送り手は、ＩＣカード１のリセットをおこなう（ステップＳ３０１）。

これによって、キーデータ領域１２、データ領域１３、キーレジスタ１４、キーデータ設定フラグ１６および暗号レジスタ１７を含む全てのメモリ領域が初期化され、ＩＣカード１の使用が可能な状態となる。

【００２６】

ついで、送り手は、データ領域１３に所望のデータを書き込む（ステップＳ３０２）。このとき、キーデータ領域１２にはキーデータが書き込まれていないので、データ領域１３は、データの書き込みおよび読み出しが可能な状態となっている。

【００２７】

データ領域１３へのデータの書き込みが終了したら、キーデータを暗号化してＩＣカード１に記憶させるか否かを選択する（ステップＳ３０３）。キーデータを暗号化しない場合には（ステップＳ３０３：Ｎｏ）、送り手は、キーデータ領域１２にキーデータを書き込む（ステップＳ３０４）。このとき、キーデータ設定フラグ１６がセットされる。これによって、データ領域１３は、データの読み出しおよび書き込みが禁止された状態となる。したがって、今後、データ領域１３へアクセスする際には、キーデータの入力が必要となる。

【００２８】

そして、送り手は、受け手にＩＣカード１を送るとともに、受け手にキーデータ２１を知らせる（ステップＳ３０５、図６参照）。なお、受け手に送るキーデータ２１を、公知の技術により暗号化しておいてもよい。その場合には、送り手は受け手に、暗号化したキーデータ２１を復号化するためのパスワードを、別途知らせる必要がある。

【００２９】

一方、キーデータを暗号化する場合には（ステップＳ３０３：Ｙｅｓ）、送り手は、たとえば受け手が公開している公開鍵を用いてキーデータの暗号化処理をおこない（ステップＳ３１１）、その結果得られた暗号データを暗号レジスタ１７に書き込む（ステップＳ３１２）。また、キーデータ領域１２にキーデータを書き込む（ステップＳ３１３）。そして、送り手は、受け手にＩＣカード１を送る。それによって、送り手は、受け手にＩＣカード１とともに暗号データを送る

ことができる（図７参照）。

【００３０】

キーデータを暗号化する場合について、ここまでのＩＣカード１のキーデータ領域１２、データ領域１３およびレジスタ１４，１７の変化の様子が図４（ａ）および同図（ｂ）に示されている。なお、キーデータを暗号化しない場合には、図４（ａ）において暗号レジスタ１７への暗号データの書き込みがおこなわれないため、図４（ｂ）において暗号レジスタ１７は空（意味のあるデータが格納されていない状態）となる。

【００３１】

受け手がＩＣカード１を受け取った段階では、データ領域１３はデータの読み出しおよび書き込みが禁止された状態となっている（図５（ａ）参照）。暗号レジスタ１７に暗号データが書き込まれている場合には、受け手は、たとえば公開鍵に対する秘密鍵を用いて暗号化を解除（暗号データを復号化）し、キーデータを取得する（ステップＳ３１４）。そして、キーレジスタ１４に、その復号化されたキーデータを書き込む（ステップＳ３０６）。

【００３２】

一方、受け手が、ＩＣカード１の他に、キーデータ２１を受け取った場合には、キーレジスタ１４にそのキーデータ２１を書き込む（ステップＳ３０６）。その際、キーデータ２１が暗号化されている場合には、受け手は、送り手から受け取ったパスワードを用いてキーデータ２１を復号化しておく。このときのＩＣカード１のキーデータ領域１２、データ領域１３およびレジスタ１４，１７の様子が図５（ａ）に示されている。

【００３３】

受け手によりキーレジスタ１４にキーデータが書き込まれると、ＩＣカード１は、キーデータ領域１２に書き込まれているキーデータと、キーレジスタ１４にキーデータとしてセットされたデータとが一致するか否かの判定をおこなう（ステップＳ３０７）。一致すれば（ステップＳ３０７：Ｙｅｓ）、ＩＣカード１は、受け手がデータ領域１３へアクセスするのを許可する。それによって、受け手は、データ領域１３からデータを読み込みできる（ステップＳ３０８）。また、

受け手は、データ領域１３にデータを書き込むこともできる。この状態が図５（ｂ）に示されている。一方、不一致の場合には（ステップＳ３０７：Ｎｏ）、ＩＣカード１は、データ領域１３へのアクセスを禁止し、受け手がデータ領域１３からデータを読み出すのを拒否する（ステップＳ３０９）。

【００３４】

データ領域１３へのアクセスが許可され、データ領域１３に対するデータの読み出しまたは書き込みが終了した後、再びデータ領域１３をアクセス禁止状態にする場合には、受け手は、キーレジスタ１４に、キーデータ領域１２に書き込まれているキーデータと異なる任意のデータを書き込む。それによって、データ領域１３に対するデータの読み出しおよび書き込みが禁止される。この状態が図５（ｃ）および同図（ｄ）に示されている。

【００３５】

上述した実施の形態１によれば、外部からキーデータとして入力されたデータと、あらかじめキーデータ領域１２に格納されているキーデータとが一致したときにのみ、ＩＣカード１のメモリ１１のデータ領域１３に対するアクセスが許可されるので、正しいキーデータを知っている者以外が、データ領域１３に記憶された秘密データを盗み見したり、改ざんしたりすることを防ぐことができる。

【００３６】

また、実施の形態１によれば、データ領域１３に、暗号化していないデータを記憶させることができるので、データの暗号化および復号化の処理が不要となり、データ領域１３に対するデータの読み出しおよび書き込みの処理を高速におこなうことができる。したがって、航空貨物に添付されるタグの代わりにＩＣカード１を用いても、ＩＣカード１が移動しながらゲートを通過するわずかな時間に、ＩＣカード１に所望の情報を書き込んだり、読み出したりすることができる。

【００３７】

また、実施の形態１によれば、ＩＣカード１のメモリ１１のキーデータ領域１２に対しては、データの書き込みは可能であるが、読み出しができないので、キーデータ領域１２からキーデータが漏洩するのを防ぐことができる。

【００３８】

（実施の形態２）

実施の形態２は、実施の形態１と同様の構成のＩＣカードに対するアクセス方法の他の例である。ＩＣカードの構成およびＩＣカードへのアクセス制限システムの構成は実施の形態１と同じであるので、それらについては、実施の形態２の説明においても実施の形態１と同じ符号を用いる。

【００３９】

図８は、実施の形態２にかかるＩＣカードへのアクセス方法を説明するフローチャートである。また、図９は、そのアクセス方法の実行時のメモリ状態を示す模式図である。

【００４０】

まず、送り手は、ＩＣカード１のリセットをおこない、ＩＣカード１を使用可能な状態とする（ステップＳ８０１）。このとき、キーデータ領域１２、データ領域１３、キーレジスタ１４、キーデータ設定フラグ１６および暗号レジスタ１７を含む全てのメモリ領域が初期化される。

【００４１】

ついで、送り手は、キーデータ領域１２にキーデータを書き込む（ステップＳ８０２、図９（ａ）参照）。このとき、キーデータ設定フラグ１６がセットされる。以後、データ領域１３へのアクセスが禁止された状態となる。ついで、送り手は、データ領域１３にデータを書き込むために、キーレジスタ１４にキーデータを入力する（ステップＳ８０３、図９（ｂ）参照）。

【００４２】

キーレジスタ１４にキーデータが入力されると、ＩＣカード１は、キーデータ領域１２に書き込まれているキーデータと、キーレジスタ１４にキーデータとしてセットされたデータとが一致するか否かの判定をおこなう（ステップＳ８０４）。一致すれば（ステップＳ８０４：Ｙｅｓ）、データ領域１３へのアクセスが許可されるので、送り手は、データ領域１３に所望のデータを書き込む（ステップＳ８０５、図９（ｃ）参照）。不一致の場合には（ステップＳ８０４：Ｎｏ）、ＩＣカード１は、データ領域１３へのアクセスを拒否する（ステップＳ８０６）。

【００４３】

データ領域１３へのデータの書き込みが終了したら、暗号化の有無を判断する（ステップＳ８０７）。暗号化をおこなわない場合には（ステップＳ８０７：Ｎｏ）、キーデータ領域１２にセットされているキーデータを消去するため、送り手は、キーデータ領域１２に、キーデータとは異なる任意のデータを書き込む（ステップＳ８０８、図９（ｃ）参照）。これによって、キーレジスタ１４に新たにセットされたデータが、キーデータ領域１２に書き込まれているキーデータと一致しなくなるので、再びデータ領域１３へのアクセスが禁止された状態となる。また、キーデータ領域１２に書き込まれているキーデータがわからなくなる。したがって、これ以降は、キーデータを知る者以外がデータ領域１３へアクセスすることができなくなる。

【００４４】

ステップＳ８０７以降は、実施の形態１（図３）のステップＳ３０３～ステップＳ３１４と同じである。したがって、実施の形態１のステップＳ３０３、ステップＳ３０４、ステップＳ３０５、ステップＳ３０６、ステップＳ３０７、ステップＳ３０８、ステップＳ３０９、ステップＳ３１０、ステップＳ３１１、ステップＳ３１２、ステップＳ３１３およびステップＳ３１４を、それぞれステップＳ８０７、ステップＳ８０８、ステップＳ８０９、ステップＳ８１０、ステップＳ８１１、ステップＳ８１２、ステップＳ８１３、ステップＳ８２１、ステップＳ８２２、ステップＳ８２３およびステップＳ８２４と読み替えて、ステップＳ８０７～ステップＳ８２４の説明とする。

【００４５】

なお、図９（ｃ）および同図（ｄ）には、キーデータを暗号化する場合のキーデータ領域１２、データ領域１３および暗号レジスタ１７の変化の様子が示されている。しかし、キーデータを暗号化しない場合には、図９（ｃ）において暗号レジスタ１７への暗号データの書き込みがおこなわれないので、図９（ｄ）において暗号レジスタ１７は空（意味のあるデータが格納されていない状態）となる。

【００４６】

上述した実施の形態２によれば、実施の形態１と同様に、データ領域１３に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域１３に対するデータの読み出しおよび書き込みが高速化されるという効果と、ＩＣカード１からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【００４７】

（実施の形態３）

実施の形態３は、実施の形態１と同様の構成のＩＣカードにおいて、データ領域１３が複数のサブデータ領域に分割され、そのサブデータ領域ごとにアクセスが制限される場合のアクセス方法の一例である。特に限定しないが、ここでは、図１０に示すように、データ領域１３がＡとＢの２つのサブデータ領域（Ａサブデータ領域１３１およびＢサブデータ領域１３２とする）に分割されていると仮定して説明する。

【００４８】

実施の形態３では、図１０に示すように、ＩＣカードには、Ａサブデータ領域１３１に対応する第１のキーデータ領域１２１と、Ｂサブデータ領域１３２に対応する第２のキーデータ領域１２２が設けられている。また、キーレジスタ１４１，１４２、図示しないキーデータ設定フラグおよび暗号レジスタ１７１，１７２も２個ずつ設けられている。それ以外のＩＣカードの構成、およびＩＣカードへのアクセス制限システムの構成は実施の形態１と同じであるので、実施の形態３の説明においても実施の形態１と同じ符号を用いる。

【００４９】

つぎに、上述した構成のＩＣカードへのアクセス方法について説明する。図１１は、実施の形態３にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【００５０】

まず、送り手は、ＩＣカード１のリセットにより、キーデータ領域１２１，１２２、サブデータ領域１３１，１３２、キーレジスタ１４１，１４２、キーデータ設定フラグ１６および暗号レジスタ１７１，１７２を含む全てのメモリ領域を

初期化して、ＩＣカード１を使用可能な状態とする（ステップＳ１１０１）。

【００５１】

ついで、送り手は、データ領域１３をＡサブデータ領域１３１とＢサブデータ領域１３２に分割する（ステップＳ１１０２）。この場合、たとえばＡサブデータ領域１３１とその先頭アドレス、およびＢサブデータ領域１３２とその先頭アドレスの対応関係を示すテーブルが、たとえばメモリ１１の所定の領域に作成される。

【００５２】

ついで、送り手は、Ａサブデータ領域１３１およびＢサブデータ領域１３２の一方または両方に所望のデータを書き込む（ステップＳ１１０３）。ついで、キーデータを暗号化してＩＣカード１に記憶させるか否かを選択する（ステップＳ１１０４）。キーデータを暗号化しない場合には（ステップＳ１１０４：Ｎｏ）、送り手は、キーデータ領域１２１，１２２にキーデータを書き込む（ステップＳ１１０５）。その際、Ａサブデータ領域１３１（またはＢサブデータ領域１３２）のアクセスだけを制限し、Ｂサブデータ領域１３２（またはＡサブデータ領域１３１）には自由にアクセスできるようにしたい場合には、Ａサブデータ領域１３１に対応するキーデータ領域１２１（またはＢサブデータ領域１３２に対応するキーデータ領域１２２）にだけキーデータを書き込めばよい。

【００５３】

Ａサブデータ領域１３１およびＢサブデータ領域１３２の両方ともアクセスを制限する場合には、両方のキーデータ領域１２１，１２２にキーデータを書き込めばよい。両方のキーデータ領域１２１，１２２に書き込むキーデータは、同じであってもよいし、異なっていてもよい。キーデータが異なっていれば、Ａサブデータ領域１３１へのアクセスとＢサブデータ領域１３２へのアクセスを独立して制限することができる。

【００５４】

キーデータの書き込みとともに、キーデータ設定フラグ１６がセットされ、以後、キーデータが設定されたサブデータ領域１３１，１３２へのアクセスが禁止された状態となる。送り手は、受け手にＩＣカード１を送るとともに、受け手に

キーデータとそれに対応するサブデータ領域を知らせる（ステップＳ１１０６）。

【００５５】

一方、キーデータを暗号化する場合には（ステップＳ１１０４：Ｙｅｓ）、送り手は、キーデータを暗号化し（ステップＳ１１１１）、暗号レジスタ１７１，１７２に書き込む（ステップＳ１１１２）。そして、キーデータ領域１２１，１２２にキーデータを書き込む（ステップＳ１１１３）。Ａサブデータ領域１３１に対応する暗号データは、Ａサブデータ領域１３１に対応する暗号レジスタ１７１に書き込まれる。同様に、Ｂサブデータ領域１３２に対応する暗号データは、Ｂサブデータ領域１３２に対応する暗号レジスタ１７２に書き込まれる。そして、送り手は、受け手にＩＣカード１を送る。

【００５６】

暗号レジスタ１７１，１７２に暗号データが書き込まれている場合には、受け手は、暗号化を解除（暗号データを復号化）してキーデータを取得する（ステップＳ１１１４）。そして、キーレジスタ１４１，１４２に、復号化されたキーデータのうちの対応するデータを書き込む（ステップＳ１１０７）。一方、受け手が、ＩＣカード１の他に、キーデータを受け取った場合には、キーレジスタ１４１，１４２に、対応するキーデータを書き込む（ステップＳ１１０７）。

【００５７】

ついで、ＩＣカード１は、キーデータの照合をおこない（ステップＳ１１０８）、キーデータが一致した場合（ステップＳ１１０８：Ｙｅｓ）、一致したキーデータに対応するサブデータ領域１３１，１３２へのアクセスを許可する。それによって、受け手は、アクセスが許可されたサブデータ領域１３１，１３２からデータを読み込みできる（ステップＳ１１０９）。一方、キーデータが一致しない場合（ステップＳ１１０８：Ｎｏ）、その一致しないキーデータに対応するサブデータ領域１３１，１３２へのアクセスが禁止され、受け手のアクセスが拒否される（ステップＳ１１１０）。

【００５８】

上述した実施の形態３によれば、複数のサブデータ領域１３１，１３２に対し

て独立してアクセスを制限することができる。また、実施の形態１と同様に、データ領域１３に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域１３に対するデータの読み出しおよび書き込みが高速化されるという効果と、ＩＣカード１からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【００５９】

（実施の形態４）

実施の形態４は、実施の形態３と同様に、実施の形態１と同様の構成のＩＣカードにおいて、データ領域１３が複数のサブデータ領域に分割され、そのサブデータ領域ごとにアクセスが制限される場合のアクセス方法の他の例である。実施の形態４が実施の形態３と異なるのは、データ領域１３に書き込まれるデータの長さに応じて、個々のサブデータ領域の大きさが設定されることである。

【００６０】

つまり、実施の形態３では、個々のサブデータ領域の大きさは固定である。それに対して、実施の形態４では、個々のサブデータ領域の大きさは可変である。また、データ領域１３に設けられるサブデータ領域の数も可変であり、データ領域１３の空き記憶容量がゼロまたはおおよそゼロになるまで、サブデータ領域の数を増やすことができる。

【００６１】

特に限定しないが、ここでは、図１２に示すように、データ領域１３がＡとＢとＣの３つのサブデータ領域（Ａサブデータ領域１３３、Ｂサブデータ領域１３４およびＣサブデータ領域１３５とする）に分割されると仮定して説明する。

【００６２】

実施の形態４では、図１２に示すように、ＩＣカードには、Ａサブデータ領域１３３に対応する第１のキーデータ領域１２３、Ｂサブデータ領域１３４に対応する第２のキーデータ領域１２４、およびＣサブデータ領域１３５に対応する第３のキーデータ領域１２５が設けられている。また、キーレジスタ１４３，１４４，１４５、図示しないキーデータ設定フラグおよび暗号レジスタ１７３，１７４，１７５も３個ずつ設けられている。

【００６３】

ただし、キーデータ領域１２３，１２３，１２５、キーレジスタ１４３，１４４，１４５、図示しないキーデータ設定フラグおよび暗号レジスタ１７３，１７４，１７５は、３個ずつに限らず、データ領域１３に設けることのできるサブデータ領域の想定される最大数まで設定可能である。それ以外のＩＣカードの構成、およびＩＣカードへのアクセス制限システムの構成は実施の形態１と同じであるので、実施の形態４の説明においても実施の形態１と同じ符号を用いる。

【００６４】

つぎに、上述した構成のＩＣカードへのアクセス方法について説明する。図１３は、実施の形態４にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【００６５】

まず、送り手は、ＩＣカード１のリセットにより、キーデータ領域１２３，１２４，１２５、サブデータ領域１３３，１３４，１３５、キーレジスタ１４３，１４４，１４５、キーデータ設定フラグ１６および暗号レジスタ１７３，１７４，１７５を含む全てのメモリ領域を初期化して、ＩＣカード１を使用可能な状態とする（ステップＳ１３０１）。

【００６６】

ついで、送り手は、データ領域１３に所望のデータを書き込む（ステップＳ１３０２）。このとき、あるデータの書き込みが完了するごとに（ステップＳ１３０３）、そのデータの格納にデータ領域１３のどこまでの領域（ブロック）を使用したかを明示するための終了印を書き込む（ステップＳ１３０４）。

【００６７】

これを図１２に示す例で説明すると、Ａサブデータ領域１３３は、データ領域１３の先頭から符号１３６で示す第１の終了印までの領域である。Ｂサブデータ領域１３４は、第１の終了印１３６のつぎのブロックから符号１３７で示す第２の終了印までの領域である。Ｃサブデータ領域１３５は、第２の終了印１３７のつぎのブロックから符号１３８で示す第３の終了印までの領域である。

【００６８】

ついで、キーデータを暗号化してＩＣカード１に記憶させるか否かを選択する（ステップＳ１３０５）。キーデータを暗号化しない場合には（ステップＳ１３０５：Ｎｏ）、ついで、送り手は、キーデータ領域１２３，１２４，１２５にそれぞれキーデータを書き込む（ステップＳ１３０６）。その際、Ａサブデータ領域１３３、Ｂサブデータ領域１３４およびＣサブデータ領域１３５の三つの領域に限らず、実施の形態３と同様に、いずれか一つまたは二つの領域だけに対してアクセスを制限し、残りの領域については自由にアクセスできるようにしてもよい。その場合には、実施の形態３と同様に、アクセスを制限する領域に対してのみ、キーデータ領域１２３，１２４，１２５にキーデータを書き込めばよい。

【００６９】

キーデータの書き込みとともに、キーデータ設定フラグ１６がセットされ、以後、キーデータが設定されたサブデータ領域１３３，１３４，１３５へのアクセスが禁止された状態となる。送り手は、受け手にＩＣカード１を送るとともに、受け手にキーデータとそれに対応するサブデータ領域を知らせる（ステップＳ１３０７）。

【００７０】

一方、キーデータを暗号化する場合には（ステップＳ１３０５：Ｙｅｓ）、送り手は、キーデータを暗号化し（ステップＳ１３１３）、暗号レジスタ１７３，１７４，１７５にそれぞれのサブデータ領域１３３，１３４，１３５に対応する暗号データを書き込む（ステップＳ１３１４）。送り手は、キーデータ領域１２３，１２４，１２５にそれぞれキーデータを書き込む（ステップＳ１３１５）。そして、送り手は、受け手にＩＣカード１を送る。

【００７１】

暗号レジスタ１７３，１７４，１７５に暗号データが書き込まれている場合には、受け手は、暗号化を解除（暗号データを復号化）してキーデータを取得する（ステップＳ１３１６）。そして、キーレジスタ１４３，１４４，１４５に、復号化されたキーデータのうちの対応するデータを書き込む（ステップＳ１３０８）。一方、受け手が、ＩＣカード１の他に、キーデータを受け取った場合には、キーレジスタ１４３，１４４，１４５に、対応するキーデータを書き込む（ステ

ップＳ１３０８）。

【００７２】

ついで、ＩＣカード１は、キーデータの照合をおこない（ステップＳ１３０９）、キーデータが一致した場合（ステップＳ１３０９：Ｙｅｓ）、一致したキーデータに対応するサブデータ領域１３３，１３４，１３５へのアクセスを許可する。受け手が、アクセスが許可されたサブデータ領域１３３，１３４，１３５のいずれかにアクセスすると、ＩＣカード１は、そのアクセスされたサブデータ領域１３３，１３４，１３５を検索して求める。具体的には、ＩＣカード１は、そのアクセスされたサブデータ領域１３３，１３４，１３５の終了印と、その一つ前の終了印を見つけ、その間の領域のデータにアクセスする（ステップＳ１３１０）。

【００７３】

これを図１２に示す例を用いて、たとえばＢサブデータ領域１３４へのアクセスが許可され、受け手がＢサブデータ領域１３４へアクセスする場合について説明する。ＩＣカード１は、Ｂサブデータ領域１３４の終了印である第２の終了印１３７と、その一つ前のＡサブデータ領域１３３の終了印である第１の終了印１３６を見つける。そして、ＩＣカード１は、第１の終了印１３６のつぎのブロックから第２の終了印１３７を含むブロックまでの領域にアクセスする。

【００７４】

このようにして、受け手は、アクセスが許可されたサブデータ領域１３３，１３４，１３５からデータを読み込みできる（ステップＳ１３１１）。一方、キーデータが一致しない場合（ステップＳ１３０９：Ｎｏ）、その一致しないキーデータに対応するサブデータ領域１３３，１３４，１３５へのアクセスが禁止され。受け手のアクセスが拒否される（ステップＳ１３１２）。

【００７５】

なお、各サブデータ領域１３３，１３４，１３５の末尾に終了印１３６，１３７，１３８を書き込み、終了印１３６，１３７，１３８を目印にしてＩＣカード１がサブデータ領域１３３，１３４，１３５にアクセスする代わりに、各サブデータ領域１３３，１３４，１３５とそのアドレスとの対応関係を示すテーブルを

、たとえばメモリ１１の所定の領域に作成し、このテーブルに基づいてサブデータ領域１３３，１３４，１３５にアクセスする構成としてもよい。

【００７６】

上述した実施の形態４によれば、複数のサブデータ領域１３３，１３４，１３５に対して独立してアクセスを制限することができる。また、実施の形態１と同様に、データ領域１３に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域１３に対するデータの読み出しおよび書き込みが高速化されるという効果と、ＩＣカード１からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【００７７】

（付記１）データの読み出しおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第１のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域と、

前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みをおこなう制御部と、

を具備することを特徴とするメモリ装置。

【００７８】

（付記２）前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとを比較する比較部をさらに具備することを特徴とする付記１に記載のメモリ装置。

【００７９】

（付記３）前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第

１のデータ領域に対するデータの読み出しおよび書き込みを禁止することを特徴とする付記２に記載のメモリ装置。

【００８０】

（付記４）データの読み出しおよび書き込みが可能で、前記第２のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第４のデータ領域をさらに具備することを特徴とする付記１～３のいずれか一つに記載のメモリ装置。

【００８１】

（付記５）前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータが一致するときに前記第４のデータ領域に対する暗号化したデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第４のデータ領域に対する暗号化したデータの読み出しのみを許可し、書き込みは禁止することを特徴とする付記４に記載のメモリ装置。

【００８２】

（付記６）前記第２のデータ領域にデータが格納されたときにセットされ、リセット時にクリアされる第５のデータ領域をさらに具備することを特徴とする付記１～５のいずれか一つに記載のメモリ装置。

【００８３】

（付記７）前記第１のデータ領域に書き込まれるデータ、前記第２のデータ領域に書き込まれるデータ、および前記第３のデータ領域に書き込まれるデータが外部から入力されるとともに、前記第１のデータ領域から読み出されたデータを外部へ出力する通信部をさらに具備することを特徴とする付記１～６のいずれか一つに記載のメモリ装置。

【００８４】

（付記８）前記通信部を介して外部から供給される電力により駆動されることを特徴とする付記１～７のいずれか一つに記載のメモリ装置。

【００８５】

（付記９）前記第１のデータ領域は、複数のサブデータ領域に分割され、また前

記制御部は、前記第２のデータ領域にサブデータ領域ごとに格納されたデータと前記第３のデータ領域にサブデータ領域ごとに格納されたデータとが一致するときに、前記サブデータ領域ごとにデータの読み出しまたは書き込みをおこなうことを特徴とする付記１～８のいずれか一つに記載のメモリ装置。

【００８６】

（付記１０）前記第１のデータ領域および前記第２のデータ領域は、強誘電体の残留分極によってデータを保持する強誘電性メモリにより構成されていることを特徴とする付記１～９のいずれか一つに記載のメモリ装置。

【００８７】

（付記１１）データの読み出しおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第１のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第３のデータ領域、並びに前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みをおこなう制御部を備えたメモリ装置と、

前記第１のデータ領域および前記第２のデータ領域にデータを書き込む書き込み手段と、

前記書き込み手段と前記メモリ装置との間のデータの授受に供せられる第１のインターフェース手段と、

前記第３のデータ領域にデータを書き込むとともに、前記第１のデータ領域に対するデータの読み出しまたは書き込みのアクセスをおこなう読み書き手段と、

前記読み書き手段と前記メモリ装置との間のデータの授受に供せられる第２のインターフェース手段と、

を具備することを特徴とするメモリアクセス制限システム。

【００８８】

（付記１２）前記メモリ装置は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとを比較する比較部をさらに備えていることを特徴とする付記１１に記載のメモリアクセス制限システム。

【００８９】

（付記１３）前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第１のデータ領域に対するデータの読み出しおよび書き込みを禁止することを特徴とする付記１２に記載のメモリアクセス制限システム。

【００９０】

（付記１４）前記メモリ装置は、データの読み出しおよび書き込みが可能で、前記第２のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第４のデータ領域をさらに備えていることを特徴とする付記１０～１３のいずれか一つに記載のメモリアクセス制限システム。

【００９１】

（付記１５）前記比較部は、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータが一致するときに前記第４のデータ領域に対する暗号化したデータの読み出しまたは書き込みを許可し、前記第２のデータ領域に格納されたデータと前記第３のデータ領域に格納されたデータとが異なるときに前記第４のデータ領域に対する暗号化したデータの読み出しのみを許可し、書き込みは禁止することを特徴とする付記１４に記載のメモリアクセス制限システム。

【００９２】

（付記１６）前記メモリ装置は、前記第２のデータ領域にデータが格納されたときにセットされ、リセット時にクリアされる第５のデータ領域をさらに備えていることを特徴とする付記１０～１５のいずれか一つに記載のメモリアクセス制限システム。

【００９３】

（付記１７）前記メモリ装置は、前記第１のデータ領域に書き込まれるデータ、前記第２のデータ領域に書き込まれるデータ、および前記第３のデータ領域に書き込まれるデータが前記第１のインターフェース手段を介して前記書き込み手段

から入力されるとともに、前記第１のデータ領域から読み出されたデータを第２のインターフェース手段を介して前記読み書き手段へ出力する通信部をさらに具備することを特徴とする付記１０～１６のいずれか一つに記載のメモリアクセス制限システム。

【００９４】

（付記１８）前記メモリ装置は、前記通信部を介して前記第１のインターフェース手段または前記第２のインターフェース手段から供給される電力により駆動されることを特徴とする付記１０～１７のいずれか一つに記載のメモリアクセス制限システム。

【００９５】

（付記１９）前記第１のデータ領域は、複数のサブデータ領域に分割され、また前記制御部は、前記第２のデータ領域にサブデータ領域ごとに格納されたデータと前記第３のデータ領域にサブデータ領域ごとに格納されたデータとが一致するときに、前記サブデータ領域ごとにデータの読み出しまたは書き込みをおこなうことを特徴とする付記１０～１８のいずれか一つに記載のメモリアクセス制限システム。

【００９６】

（付記２０）前記第１のデータ領域および前記第２のデータ領域は、強誘電体の残留分極によってデータを保持する強誘電性メモリにより構成されていることを特徴とする付記１０～１９のいずれか一つに記載のメモリアクセス制限システム。

【００９７】

（付記２１）リセット後に、データの読み出しおよび書き込みが可能な不揮発性の第１のデータ領域に暗号化されていない所定のデータを書き込むとともに、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第２のデータ領域にキーデータを書き込み、前記第１のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態にする第１の工程と、

前記第１のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態のときに、データの書き込みが可能で、かつデータの読み出しが不可能な不

揮発性の第３のデータ領域に仮のキーデータを書き込む第２の工程と、

前記仮のキーデータが前記キーデータに一致するときに前記第１のデータ領域に対するデータの読み出しまたは書き込みを許可し、一方、前記仮のキーデータが前記キーデータと異なるときに前記第１のデータ領域に対するデータの読み出しおよび書き込みを禁止する第３の工程と、

を含むことを特徴とするメモリアクセス方法。

【００９８】

（付記２２）前記第２の工程の前に、

データの読み出しおよび書き込みが可能な不揮発性の第４のデータ領域に、前記キーデータを暗号化して書き込む第４の工程と、

前記第４のデータ領域に格納されている暗号データを読み出し、該暗号データを復号化して前記キーデータを取得する第５の工程と、

をさらに有し、

前記暗号データの復号化により得られたキーデータを、前記第２の工程において仮のキーデータとして前記第３のデータ領域に書き込むことを特徴とする付記２１に記載のメモリアクセス方法。

【００９９】

以上において本発明は、上述した各実施の形態に限らず、種々変更可能である。また、本発明にかかるメモリ装置は、荷札としてのＩＣカードに限らず、クレジットカードや、身分証明用のＩＣカードや、社員証や従業員証などのＩＣカードにも適用可能である。また、本発明にかかるシステムは、航空貨物における運搬サービスに限らず、宅配等の集荷サービスや、倉庫における保管物の管理サービスなどにも適用可能である。

【０１００】

【発明の効果】

本発明によれば、キーデータを読み出すことができず、かつ正しいキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが許可され、間違ったキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが禁止されるので、メモリ装置にデータを暗号化するこ

となく記憶させることができ、またその記憶データの漏洩や改ざんを防ぐことができるという効果を奏する。

【図面の簡単な説明】

【図１】

実施の形態１にかかるＩＣカードの構成を示すブロック図である。

【図２】

実施の形態１にかかるＩＣカードへのアクセス制限システムの概略構成を示す模式図である。

【図３】

実施の形態１にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【図４】

実施の形態１にかかるＩＣカードの初期化時のメモリ状態を示す模式図である。

【図５】

実施の形態１にかかるＩＣカードのメモリアクセス時のメモリ状態を示す模式図である。

【図６】

実施の形態１にかかるＩＣカードにおけるキーデータの授受形態の一例を示す模式図である。

【図７】

実施の形態１にかかるＩＣカードにおけるキーデータの授受形態の他の例を示す模式図である。

【図８】

実施の形態２にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【図９】

実施の形態２にかかるＩＣカードの初期化時のメモリ状態を示す模式図である。

【図１０】

実施の形態３にかかるＩＣカードのメモリマップを示す模式図である。

【図１１】

実施の形態３にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【図１２】

実施の形態４にかかるＩＣカードのメモリマップを示す模式図である。

【図１３】

実施の形態４にかかるＩＣカードへのアクセス方法を説明するフローチャートである。

【符号の説明】

１　メモリ装置（ＩＣカード）

２　書き込み手段（コンピュータ）

３　読み書き手段（コンピュータ）

４　第１のインターフェース手段（リーダ／ライタ）

５　第２のインターフェース手段（リーダ／ライタ）

１２，１２１～１２５　第２のデータ領域（キーデータ領域）

１３　第１のデータ領域（データ領域）

１３１～１３５　サブデータ領域

１４，１４１～１４５　第３のデータ領域（キーレジスタ）

１５　比較部

１６　第５のデータ領域（キーデータ設定フラグ）

１７，１７１～１７５　第４のデータ領域（暗号レジスタ）

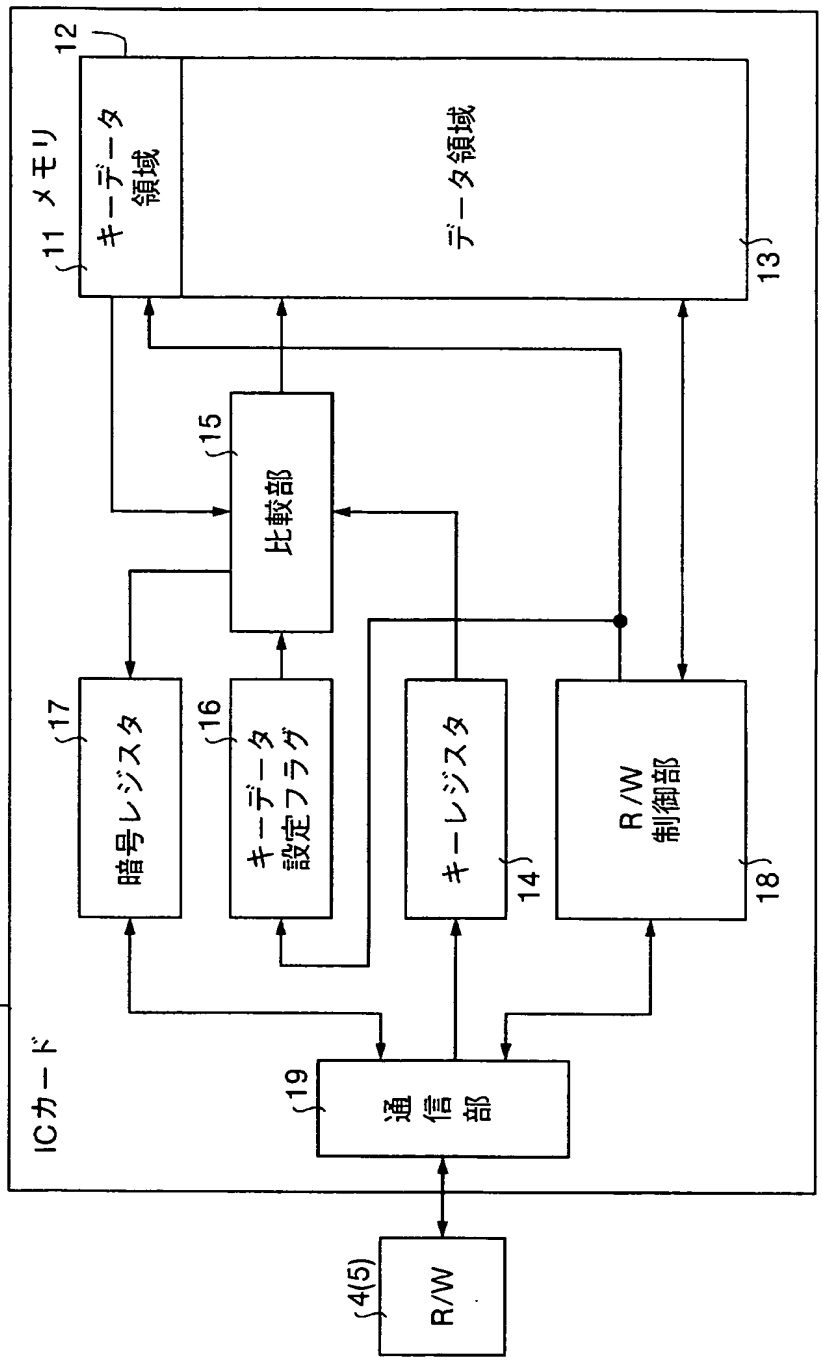
１８　制御部（リード／ライト制御部）

１９　通信部

【書類名】　図面

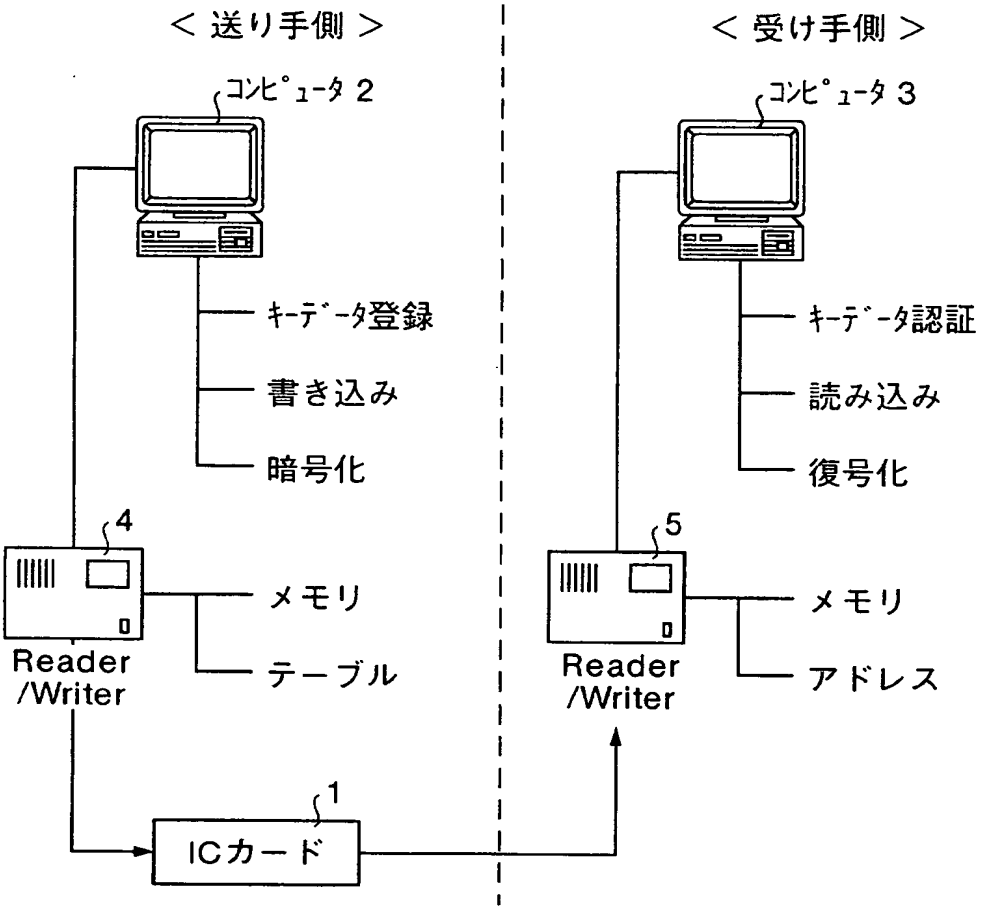
【図１】

実施の形態１にかかるＩＣカードの構成を示すブロック図



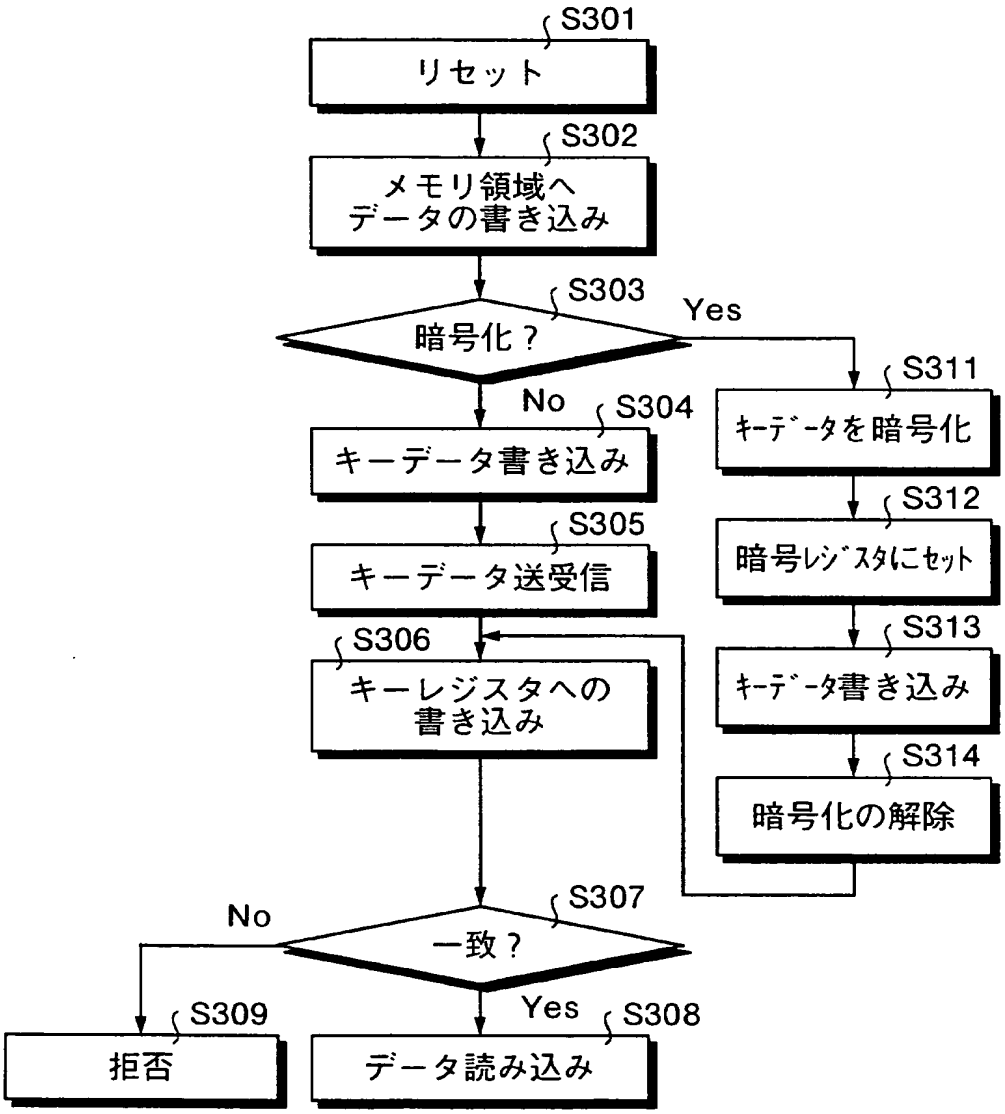
【図２】

実施の形態１にかかる
ＩＣカードへのアクセス制限システムの概略構成を示す模式図



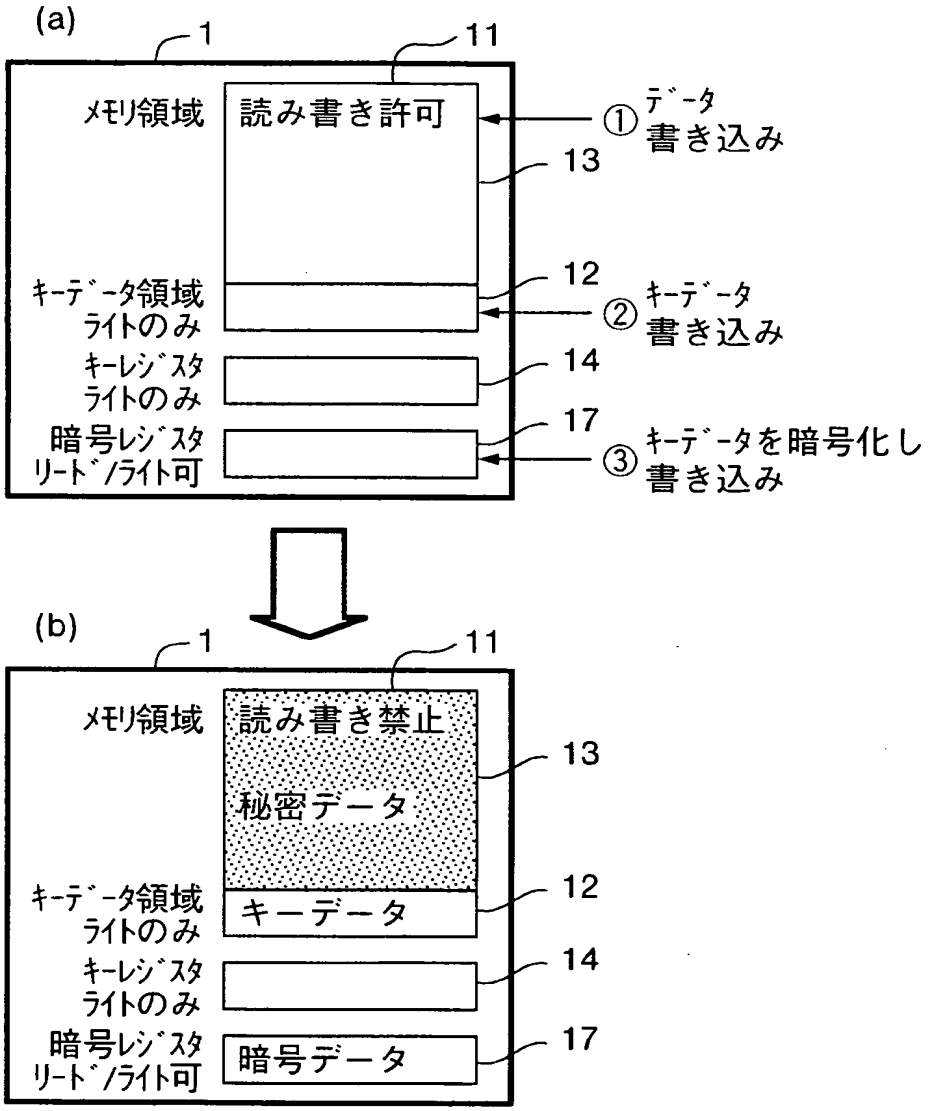
【図３】

実施の形態１にかかる
ＩＣカードへのアクセス方法を説明するフローチャート

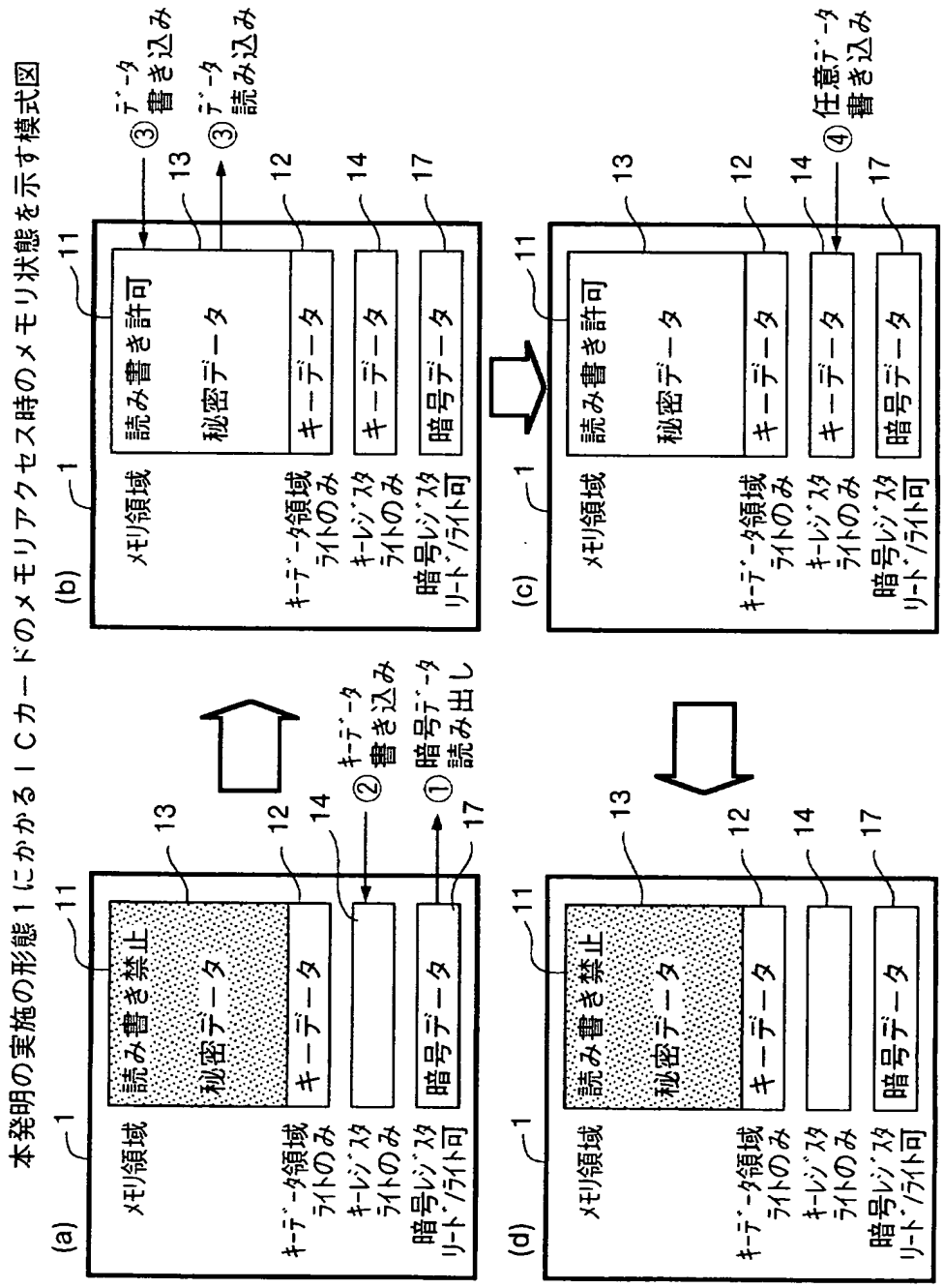


【図４】

実施の形態１にかかる
ＩＣカードの初期化時のメモリ状態を示す模式図

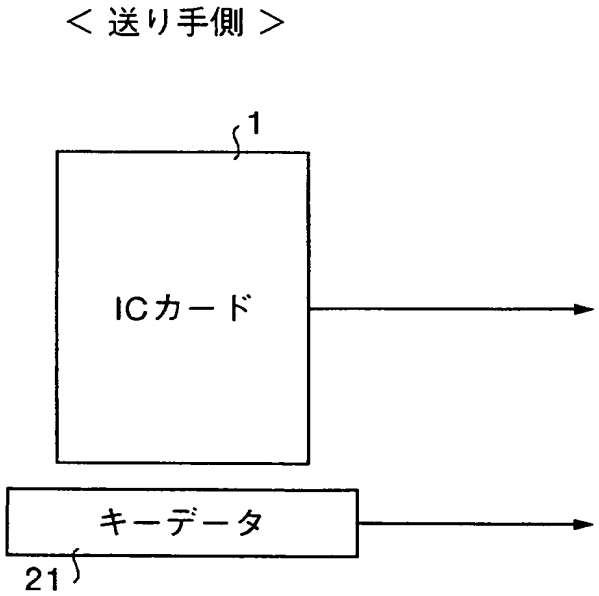


【図５】


本発明の実施の形態１にかかるＩＣカードのメモリアクセス時のメモリ状態を示す模式図
(a)
(b)
(c)
(d)
メモリ領域
読み書き禁止
秘密データ
キーデータ
暗号データ
キーデータ領域 ライトのみ
キーレジスタ ライトのみ
暗号レジスタ リード/ライト可
① 暗号データ 読み出し
② キーデータ 書き込み
③ データ 読み込み
③ データ 書き込み
④ 任意データ 書き込み
1
11
12
13
14
17

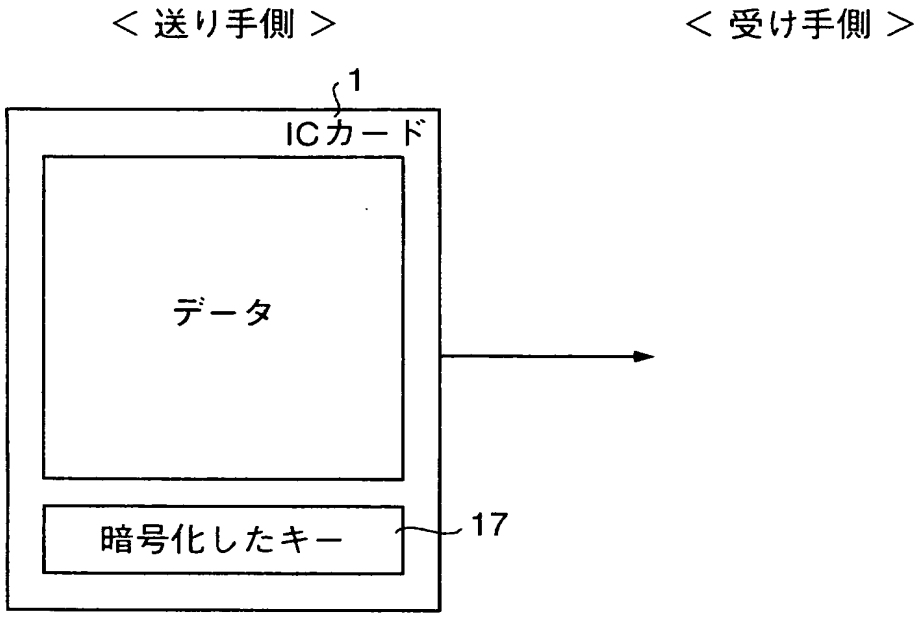
【図６】

実施の形態１にかかる
ＩＣカードにおけるキーデータの授受形態の一例を示す模式図



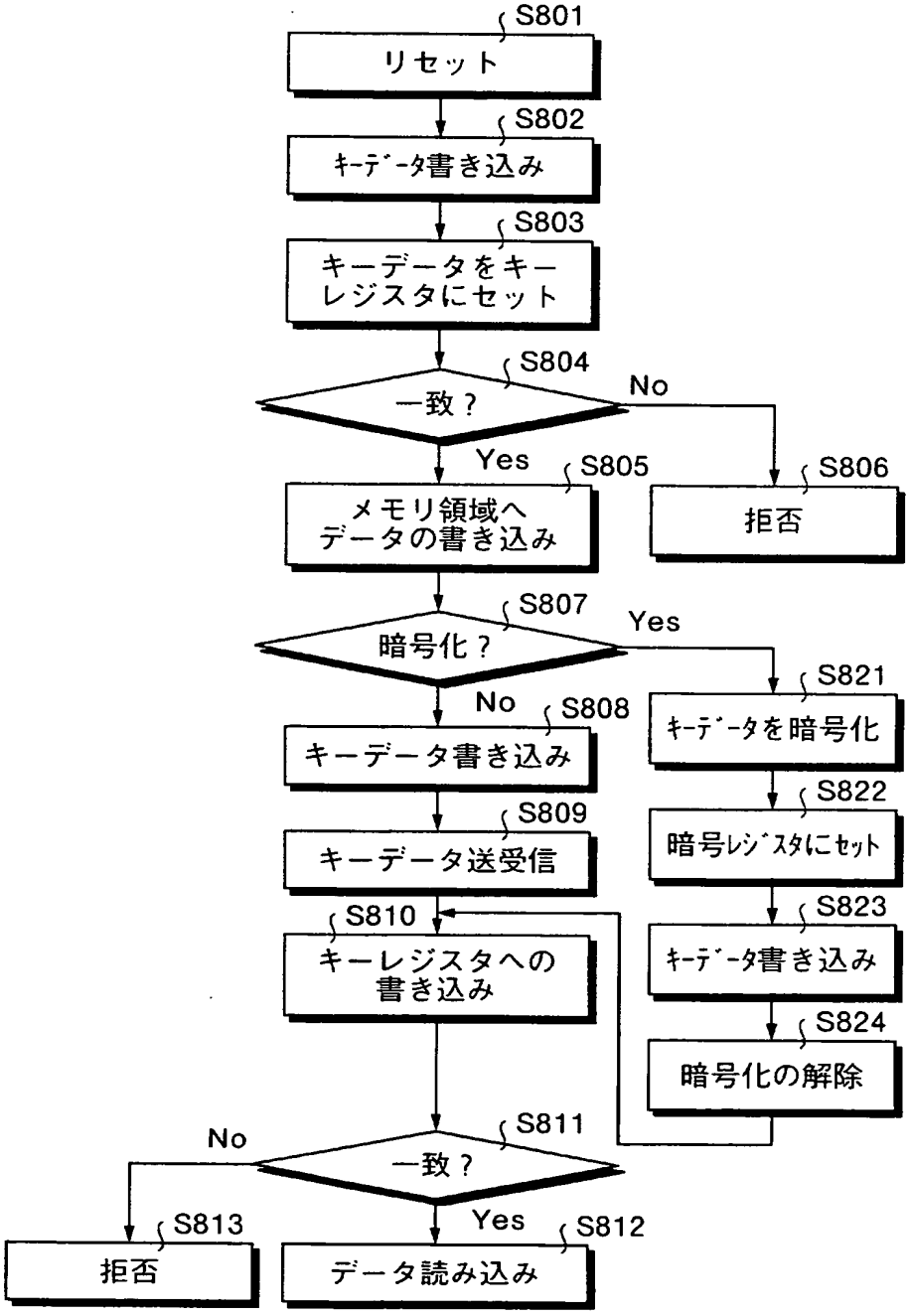
【図７】

実施の形態１にかかる
ＩＣカードにおけるキーデータの授受形態の他の例を示す模式図

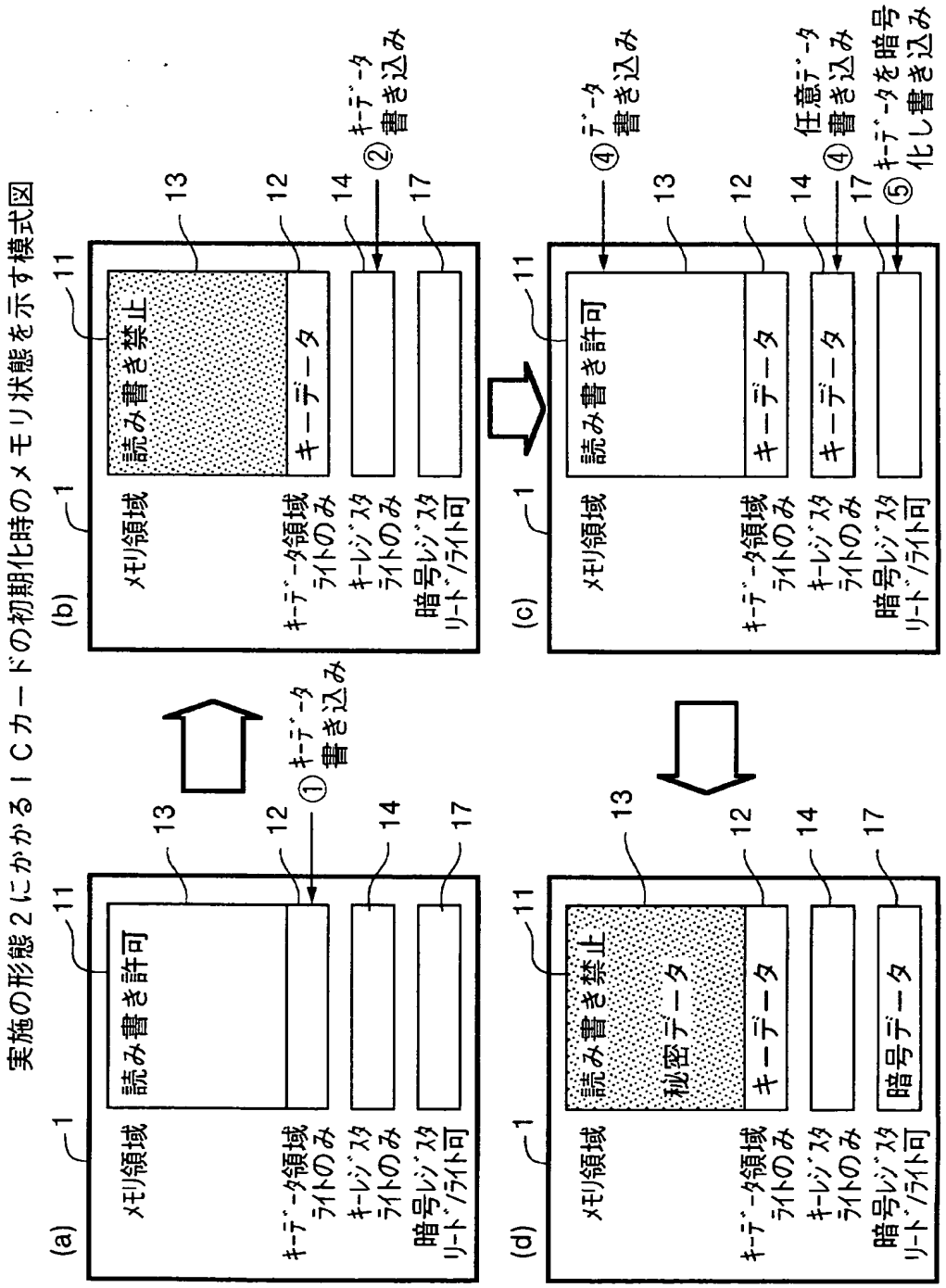


【図８】

実施の形態２にかかる
ＩＣカードへのアクセス方法を説明するフローチャート

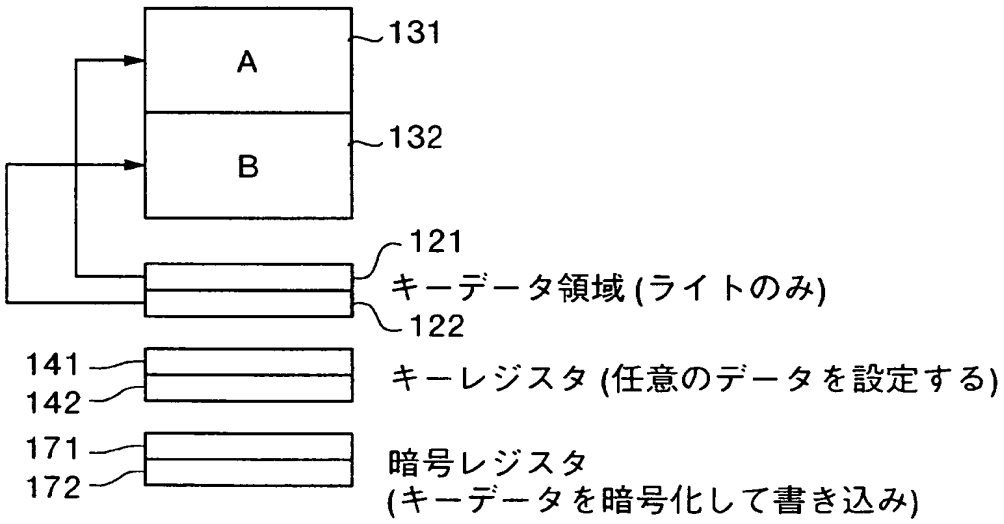


【図９】


実施の形態２にかかるＩＣカードの初期化時のメモリ状態を示す模式図
(a)
(b)
(c)
(d)
メモリ領域
読み書き許可
読み書き禁止
キーデータ
秘密データ
暗号データ
キーデータ領域 ライトのみ
キーレジスタ ライトのみ
暗号レジスタ リードのみ ライト可
① キーデータ 書き込み
② キーデータ 書き込み
④ データ 書き込み
④ 任意データ 書き込み
⑤ キーデータを暗号化し書き込み
11
12
13
14
17
1

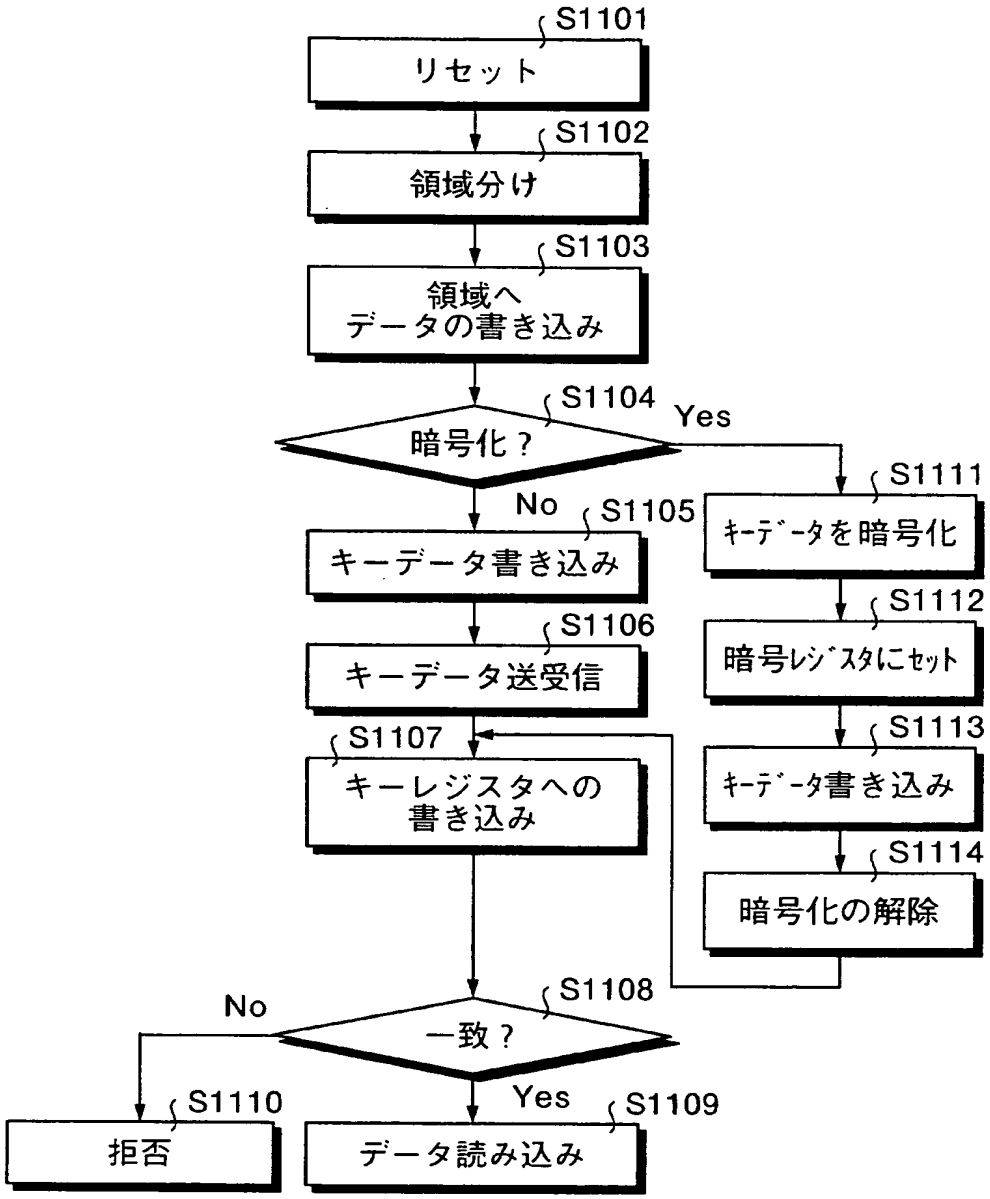
【図１０】

実施の形態３にかかるＩＣカードのメモリマップを示す模式図



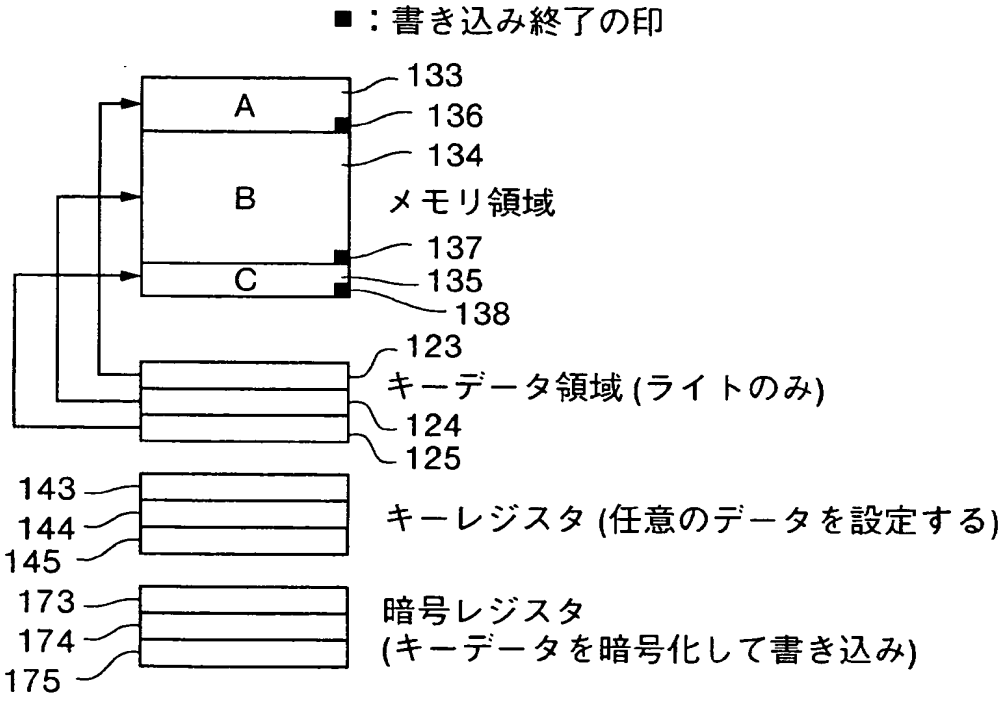
【図１１】

実施の形態３にかかる
ＩＣカードへのアクセス方法を説明するフローチャート



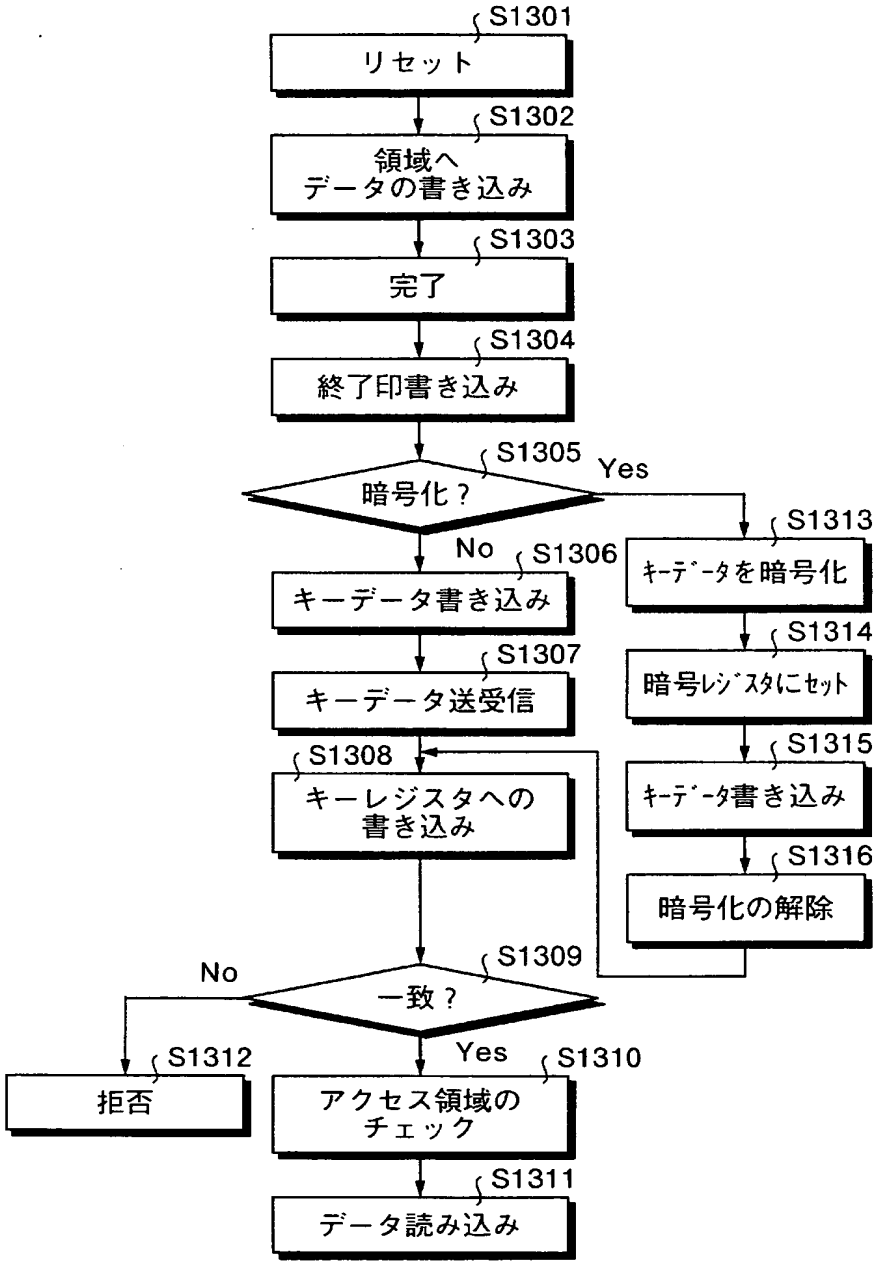
【図１２】

実施の形態４にかかるＩＣカードのメモリマップを示す模式図



【図１３】

実施の形態４にかかる
ＩＣカードへのアクセス方法を説明するフローチャート



【書類名】　　要約書

【要約】

【課題】　ＩＣカードにデータを暗号化することなく記憶させ、その記憶データの漏洩や改ざんを防ぐこと。

【解決手段】　ＩＣカード１に、データの読み出しおよび書き込みが可能な不揮発性のデータ領域１３と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性のキーデータ領域１２と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性のキーレジスタ１４を設ける。データ領域１３に暗号化されていない秘密にすべき所定のデータを書き込み、キーデータ領域１２にキーデータを書き込むことによって、データ領域１３に対するデータの読み出しおよび書き込みを禁止する。データ領域１３に対するデータの読み出しまたは書き込みを、キーレジスタ１４に正しいキーデータが書き込まれたときに許可し、間違ったキーデータが書き込まれたときに禁止する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社

特願２００３－０９７４０１

出　願　人　履　歴　情　報

識別番号　　［０００２３７１５６］

１．変更年月日　　１９９８年　４月　３日
［変更理由］　　名称変更
住　所　　東京都日野市富士町１番地
氏　名　　株式会社エフ・エフ・シー